(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 January 2001 (18.01.2001)

PCT

(10) International Publication Number
WO 01/04727 A1

(51) International Patent Classification[7]: G06F 1/00, H04N 7/16

(21) International Application Number: PCT/EP00/06371

(22) International Filing Date: 5 July 2000 (05.07.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/143,500 9 July 1999 (09.07.1999) US
09/557,599 25 April 2000 (25.04.2000) US

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors: FREEMAN, Martin; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). LU, Jin; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: GROENENDAAL, Antonius, W., M.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

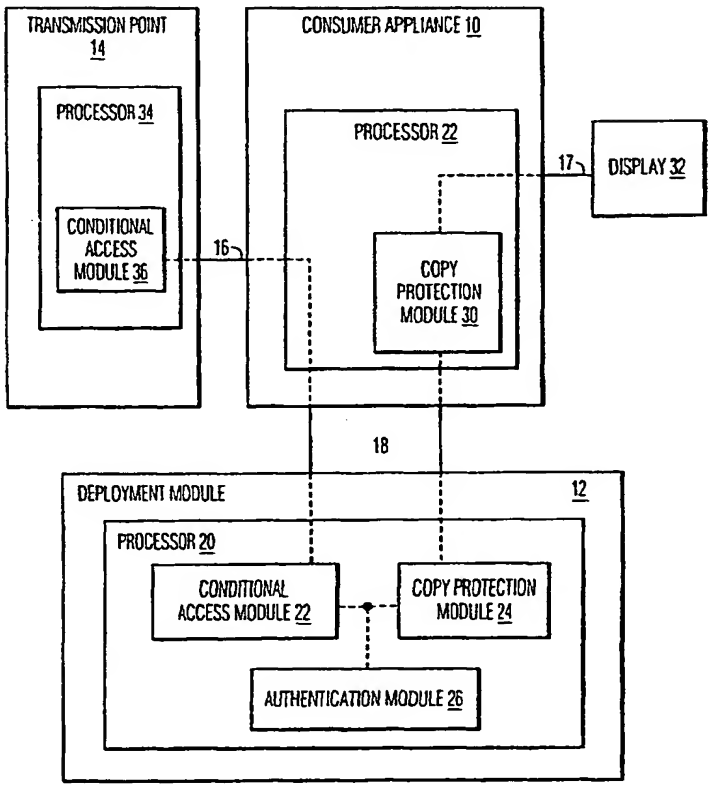
(81) Designated State *(national)*: JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: GENERALIZED CERTIFICATE PROCESSING FOR DEPLOYMENT MODULE BASED COPY PROTECTION SYSTEMS



(57) Abstract: Method and system for generalized digital certificate processing in a one-way transmission systems related to the copy protection of content transmitted between a deployment module, such as a POD module, and a consumer appliance, such as a set-top box, are disclosed by an arrangement in which a certificate authentication program code is transmitted to a deployment module on demand from a transmission point. This allows the deployment module to accommodate multiple types of certificates. In particular, the deployment module requests a digital certificate from the associated consumer appliance to retrieve a consumer appliance authentication number. Using the certificate along with information relating to the type of deployment module used, the transmission point selects an appropriate certificate authentication code and sends it to the deployment module. This authentication information is then used to complete the copy protection validation process.

WO 01/04727 A1

Generalized certificate processing for deployment module based copy protection systems

FIELD OF THE INVENTION

This invention relates to a communication system and, more particularly, to certificate processing relating to a copy protection system for information transmitted between a deployment module, such as a point of deployment (POD) module, and a consumer appliance, such as a set-top box.

BACKGROUND OF THE INVENTION

Digital transmission is used to receive and conduct numerous services and transactions, for example, to receive video, audio and data streams from a (cable television) service provider, such as Emergency Alerting, Interactive Program Guides, Impulse Pay-Per-View (IPPV), Video On Demand (VOD), General Messaging, and Interactive Services, hereinafter collectively known as "content".

Consequently, the digital transmission of content has generated the need for the copy protection of content. Recent proposed schemes for protecting digital content require appliances that receive digital content to possess digital certificates, so that these appliances may be authenticated.

Typically, some authority has the means of identifying pirate or illegal appliances, and when queried during an authentication process will evaluate the certificate and give instructions as to whether the appliance will be allowed to view copy protected content, or even, perhaps, be isolated from other authenticated appliances.

Recently, consumer appliances have become available for receiving digital content that have a separate security function embedded in a removable PC card also known a Point of Deployment (POD) Module (For additional details on POD modules, see SOCIETY OF CABLE TELECOMMUNICATIONS ENGINEERS, INC. (SCTE) Document: SCTE DVS 131 Rev. 7, entitled "Draft Point-of-Deployment (POD) Module Interface Proposal" dated December 3, 1998, (hereinafter known as "DVS131r7"). This card is part of a conditional access system, with another part residing at the transmission point of the content. A transmission point of the content is also called a head-end.

Content is scrambled at the transmission point, and then de-scrambled at the POD and then passed on to the consumer appliance itself. The conditional access system ensures that the consumer appliance only receives content for which the consumer has previously paid.

It is at the interface between the POD and its associated consumer appliance that a copy protection system must be used, otherwise even paid-for content can be copied for illegal distribution. This copy protection system also uses a scrambling/de-scrambling scheme between the POD and the consumer appliance.

In order for the copy protection scheme to be initialized, a certificate embedded in the consumer appliance must be authenticated. If this certificate either cannot be authenticated or does not pass an authentication process, the conditional access system in the POD will be instructed not to de-scramble any content, even paid-for content.

In the case of a two-way transmission system where data can be transmitted and received between a content transmission point and a POD, the transmission point can receive the certificate from a given consumer appliance for authentication and then provide instructions to the POD. In this case, any suitable digital certificate can be used, with the transmission point detecting the type of certificate and then performing the indicated computation.

However, in the case of a one-way transmission system where data can only be transmitted from the transmission point to the POD, the POD must play a greater role in the authentication process. Since the POD has fewer resources than the transmission point, heretofore it could only accommodate one certificate scheme.

In one-way transmission systems, the POD requests the certificate from the associated consumer appliance, and obtains a consumer appliance authentication number from the received certificate. Combining this number with a certificate authentication code, which is embedded in its conditional access system, the POD causes a version of this information to be displayed on the display associated with the consumer appliance.

The consumer then telephones an operator at the transmission point and relates the information displayed on the display appliance. The operator enters the information into the transmission point's computer system, and the information is used to authenticate the information supplied from the certificate.

Sometime later the transmission point sends a message to the consumer appliance's POD with authentication instructions. The POD then validates the certificate, and, if both the authentication and validation processes yield a positive result, the copy

protection scheme is initialized. If there is not a positive result, the copy protection scheme is not initialized and the POD conditional access system will not de-scramble paid-for content.

Accordingly, known practices are limited such that in one-way transmission systems the POD is only able to validate one type of certificate.

Thus, there is a clear and present need for an effective means to provide copy protection of content in one-way transmission systems that provides greater flexibility with regard to processing certificates, while minimizing additional cost and complexity.

SUMMARY OF THE INVENTION

It is an object of the present invention to generalize deployment module processing in one-way transmission systems to accommodate multiple certificate schemes with only a modest amount of cost and extra processing.

The problems associated with certificate processing in one-way transmission systems related to copy protection of content transmitted between a deployment module, such as a POD module, and a consumer appliance, such as a set-top box, are reduced or overcome by an arrangement in accordance with the principles of the present invention in which a certificate authentication code is transmitted to a deployment module on demand from a transmission point. This allows the deployment module to accommodate multiple types of certificates.

Specifically, the deployment module requests a certificate from the associated consumer appliance to retrieve a consumer appliance authentication number. Using the certificate along with information relating to the type of deployment module used, the transmission point selects an appropriate certificate authentication code and sends it to the deployment module. The authentication code includes, for example, a software program that takes a certificate as input and validates it. This transmission is protected by the existing conditional access system.

In one illustrative embodiment, the deployment module displays the authentication information on a display associated with the consumer appliance, which includes the type of certificate and information relating to the type of the deployment module. Thereafter, a user or consumer relates this authentication information to the transmission point, for example via telephone to an operator.

When the transmission point receives the above-mentioned authentication information, it decides on the authentication code that must be downloaded to the corresponding deployment module so that the deployment module can carry on the process of validating the particular

certificate on the consumer appliance. The transmission of the authentication code is protected by the existing operational conditional access system. If the certificate is valid, then the copy protection system can be initialized.

BRIEF DESCRIPTION OF THE DRAWING

The invention will be more readily understood after reading the following detailed description taken in conjunction with the accompanying drawing, in which:

FIG. 1 illustrates an exemplary system in accordance with the principles of the present invention; and

FIG. 2 illustrates the authentication component of the exemplary system in FIG.1.

DETAILED DESCRIPTION

FIG. 1 is an exemplary system according to the principles of the present invention in which generalized certificate processing for deployment module based copy protection systems is implemented. It will be recognized that FIG. 1 is simplified for explanation purposes and that the full system environment for the invention will comprise, for example, a cable, fiber or satellite service provider network or provisions for network reliability through redundancy, all of which need not be shown here. The system illustratively includes a consumer appliance 10, such as a set-top box, and a deployment module 12, such as a point of deployment (POD) module, a transmission point 14, such as a cable service provider, which communicate with each other through communication mediums 16 and 18 respectively. The communication mediums are, for example, wireless communications, electromagnetic card interfaces, optical communications, coax cables, telephone lines and the like.

Deployment module 12 includes a processor 20 that has a conditional access module 22, a copy protection module 24 and a certificate authentication module 26. Deployment module 12 communicates with consumer appliance 10 via communication medium 18.

Although deployment module 12 is described as a POD module, this arrangement is merely for convenience and it is to be understood that deployment modules are not limited to POD modules, per se. As used herein, the term "deployment module" refers to any type of (1) point of deployment module, (2) wireless, cellular or radio data interface appliance, (3) smartcard (4) personal computer, and (5) internet interface appliance,

which facilitates the transfer of data, access remote services or engage in transactions and in which privacy and/or security is desired.

Consumer appliance 10 includes a processor 22 that has a copy protection module 30. Alternatively, the copy protection module may be a separate unit coupled to processor 22. Consumer appliance 10 communicates with transmission point 14 via communication medium 16 . The display 32 associated with consumer appliance 10 is any displaying means such as a television, computer monitor, laptop computer, personal organizer (such as a Palmpilot™) and the like. Communication also occurs between display 32 and the transmission point 14, for example, when a user views what's on the display and relays the information to an operator at the transmission point via a telephone call.

As with the deployment module 12, consumer appliance 10 is not limited to any particular type device and its description as a set-top box is merely for convenience. As used herein, the term "consumer appliance" refers to any type of (1) so-called "set-top box", (2) wireless, cellular or radio data interface appliance, (3) personal computer, and (4) internet interface appliance, which: enables reception of data, allows access to remote services and facilitates remote transactions.

Transmission point 14 includes a processor 34 that has a conditional access module 36.The transmission point is any transmission facility such as a cable television service provider, Internet service/content provider, satellite service provider, television broadcast provider and the like.

The majority of logic, control, supervisory, translation functions required for the operation of deployment module 12, consumer appliance 10 and transmission point 14 is performed by their respective processors, each of which also includes programs to allow generalized certificate processing. The processor can be any of a number of commercially available processors, for example that may include dedicated digital signal processors (DSPs), a central processing unit (CPU) and memory chips.

The embodiment shown in FIG. 1 is particularly useful for generalized certificate processing of POD-based copy protection systems, wherein a POD module and a set-top box are used in a service provider communications network, such as a cable television network. In this embodiment, a conditional access system includes both conditional access modules 36 and 22, while a copy protection system includes both copy protection modules 30 and 24. However, it is to be understood that other conditional access systems and copy protection systems are equally applicable to the devices described above.

Figure 2 shows an exemplary deployment module's authentication module for use in the embodiment of FIG.1. This authentication module includes a central processing unit (CPU) 20, a random access memory (RAM) 22, a non-volatile RAM 24, and an interconnecting bus 26. The non-volatile RAM contains the instructions for most of the authentication process as well as the serial number for the embedded conditional access system. The module's CPU executes these instructions.

During the authentication process, the authentication module obtains the consumer appliance's certificate, placing it in the module's RAM. The consumer appliance's serial number is extracted from the certificate along with the certificate type and sent along with the serial number for the local conditional access system and the type of the deployment module's CPU to the display controlled by the consumer appliance.

Returning now to FIG. 1, in operation, once the copy protection system has been initialized, as part of this initialization process, the deployment module's authentication module 26 verifies a certificate obtained from consumer appliance 10. The deployment module requests a certificate from the associated consumer appliance to retrieve a consumer appliance authentication number. Using the authentication information (e.g. the certificate along with information relating to the type of deployment module used), the transmission point selects an appropriate authentication code and sends it to the deployment module.

The authentication information is sent to the transmission point in any conventional manner, for example, the deployment module displays the authentication information on a display associated with the consumer appliance. Thereafter, a user or consumer relates this authentication information to the transmission point, for example via telephone to an operator.

If the transmission point has positively authenticated the consumer appliance, it transmits a piece of authentication program code (e.g. a software program), along with other conventional authentication information, to the deployment module where the code is used by the POD to validate the certificate.. This transmission is protected by the existing operational conditional access system. If the certificate is valid, then the copy protection system can be initialized.

Specifically, content or data scrambled by conditional access module 36 in transmission point 14 is transmitted to consumer appliance 10 and from there to the deployment module 12. Within the deployment module it is de-scrambled by the deployment module conditional access module 22. Thereafter it is scrambled again by the deployment

module's copy protection module 24. The scrambled data is transmitted back to the consumer appliance 10 where its copy protection module 30 de-scrambles it.

Advantageously, by downloading the certificate authentication program code on demand from the transmission point (and not embedding the certificate authentication program code in the deployment module), the deployment module is able to operate with multiple types of certificates.

Finally, it is to be understood that although the invention is disclosed herein in the context of particular illustrative embodiments, those skilled in the art will be able to devise numerous alternative arrangements. In particular, the functions of the various elements shown in the FIGS 1 and 2, including functional blocks labeled as "processors" may be provided through the use of dedicated hardware as well as hardware capable of executing software in association with appropriate software. When provided by a processor, the functions may be provided by a single dedicated processor, by a single shared processor, or by a plurality of individual processors, some of which may be shared. Moreover, explicit use of the term "processor" or "controller" should not be construed to refer exclusively to hardware capable of executing software, and may implicitly include, without limitation, digital signal processor (DSP) hardware, read-only memory (ROM) for storing software, random access memory (RAM), and non-volatile storage. Other hardware, conventional and/or custom, may also be included. Such alternative arrangements, although not explicitly shown or described herein, embody the principles of the present invention and are thus within its spirit and scope.

CLAIMS:

1. A one-way transmission system for certificate processing relating to copy protecting, the system comprising:

a deployment module (12);

a consumer appliance (10) connected to the deployment module (12);

a transmission point (14) connected to the consumer appliance; and

wherein the deployment module (12) transmits a request to the consumer appliance (10) for a certificate, a portion of the information contained in the certificate and information relating to the type of deployment module (12) is sent to the transmission point (14), using the portion of the information contained in the certificate and information relating to the type of deployment module (12) the transmission point (14) selects a certificate authentication code and transmits it to the deployment module (12), the authentication code is used to complete a copy protection validation process.

2. The system of claim 1 wherein the authentication code includes a program for validating the certificate.

3. The system of claim 1 further including a display (32) for displaying the portion of the information contained in the certificate and information relating to the type of deployment module (12).

4. A method of processing a certificate in a one-way transmission system relating to copy protecting, the method comprising the step of:

(a) transmitting a request for a certificate from a deployment module (14) to a consumer appliance (10);

(b) sending a portion of the certificate and
information relating to the type of deployment module
to a transmission point (14);

(c) selecting an authentication program code using the portion of the certificate and the information relating to the type of deployment module;

(d) transmitting the authentication program code from the transmission point (14) to the deployment module (12); and

5. The method of claim 4 further including the step of (e) completing a copy protection validation process using the authentication program code.

6. The method of claim 4 further including the step of displaying the portion of the certificate and
information relating to the type of deployment module on a display device connected to the consumer appliance (10).

7. The method of claim 6 wherein the displaying step is used to facilitate sending the portion of the certificate and information relating to the type of deployment module to the transmission point (14) in the sending step.

8. A deployment module (12) for use in a one-way transmission system with a consumer appliance (10) and a transmission point (14), the deployment module (12) comprising:

means for communicating (20) with the consumer appliance (10); and

a processor (20) for requesting a certificate from the consumer appliance (10), and in response to the receipt of the certificate transmitting a portion of the certificate and information relating to the type of deployment module to the consumer appliance, and receiving an authentication code from the transmission point (14) selected using the portion of the certificate and the information relating to the type of deployment module.

9. The deployment module (12) of claim 8 wherein the authentication code includes a program for validating the certificate.

10. The deployment module (12) of claim 8, wherein the deployment module (12) is selected from the group consisting of a point of deployment module, wireless data interface appliance, smartcard, personal computer or internet interface appliance.

11. The deployment module (12) of claim 10, wherein the consumer appliance (10) is selected from the group consisting of a set-top box, wireless, interface appliance,

cellular interface appliance, radio interface appliance, personal computer, or internet interface appliance.

12. A consumer appliance (10) for use one-way transmission with a deployment module (12) and a transmission point (10), the consumer appliance (10) comprising:

means for communicating (20) with the deployment module; and

a processor for (20), in response to a request of a certificate, transmitting the certificate to the deployment module (12), receiving a portion of the certificate and information relating to the type of deployment module, facilitating the transfer of the portion of the certificate and information relating to the type of deployment module to a transmission point (14).

13. The consumer appliance (10) of claim 12, wherein the consumer appliance (10) is selected from the group consisting of a set-top box, wireless, interface appliance, cellular interface appliance, radio interface appliance, personal computer, or internet interface appliance.

14. The consumer appliance (10) of claim 14, further including a display (32) for displaying portion of the certificate and information relating to the type of deployment module.

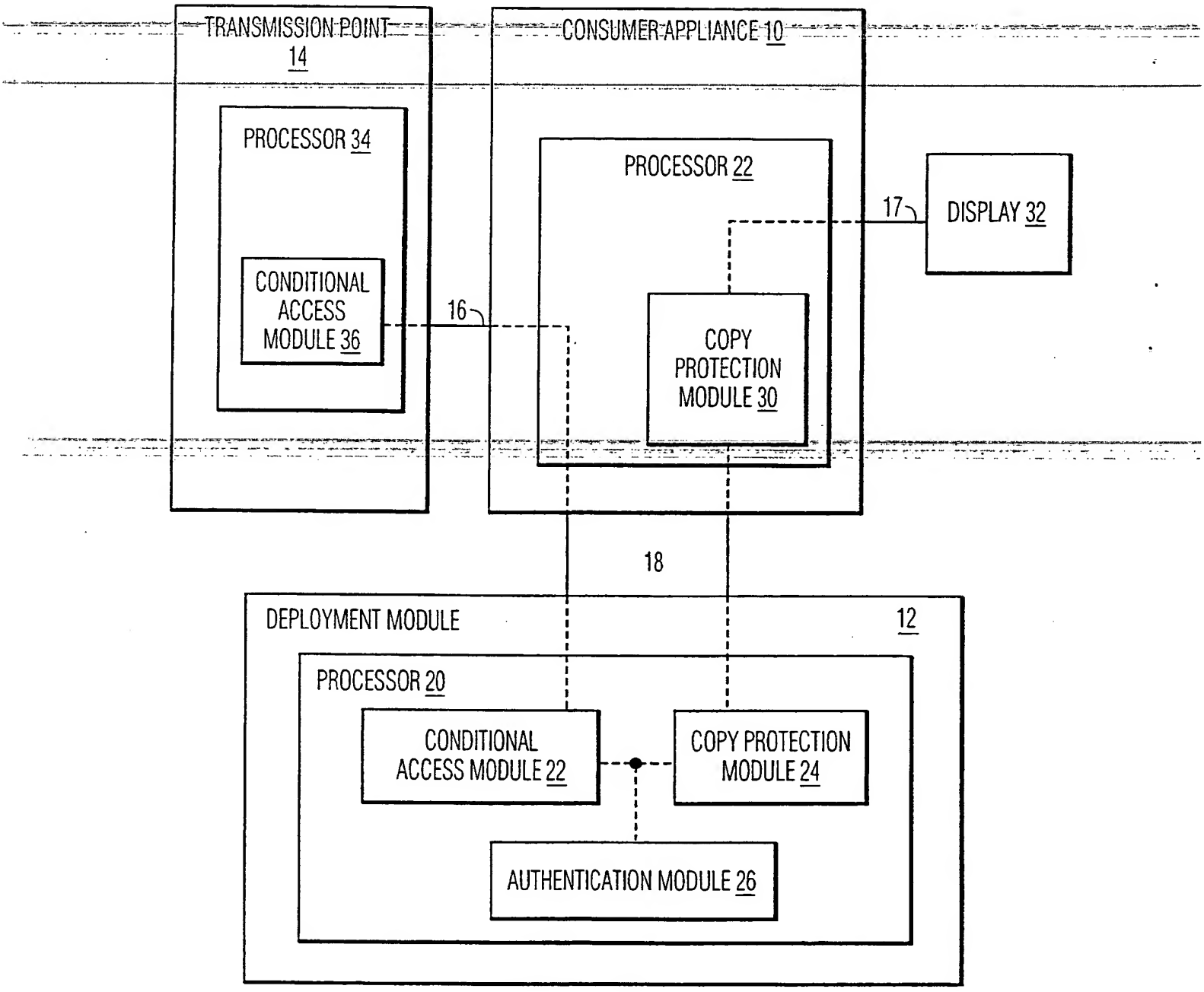

TRANSMISSION POINT 14
PROCESSOR 34
CONDITIONAL ACCESS MODULE 36
16
CONSUMER APPLIANCE 10
PROCESSOR 22
17
DISPLAY 32
COPY PROTECTION MODULE 30
18
DEPLOYMENT MODULE
12
PROCESSOR 20
CONDITIONAL ACCESS MODULE 22
COPY PROTECTION MODULE 24
AUTHENTICATION MODULE 26

FIG. 1

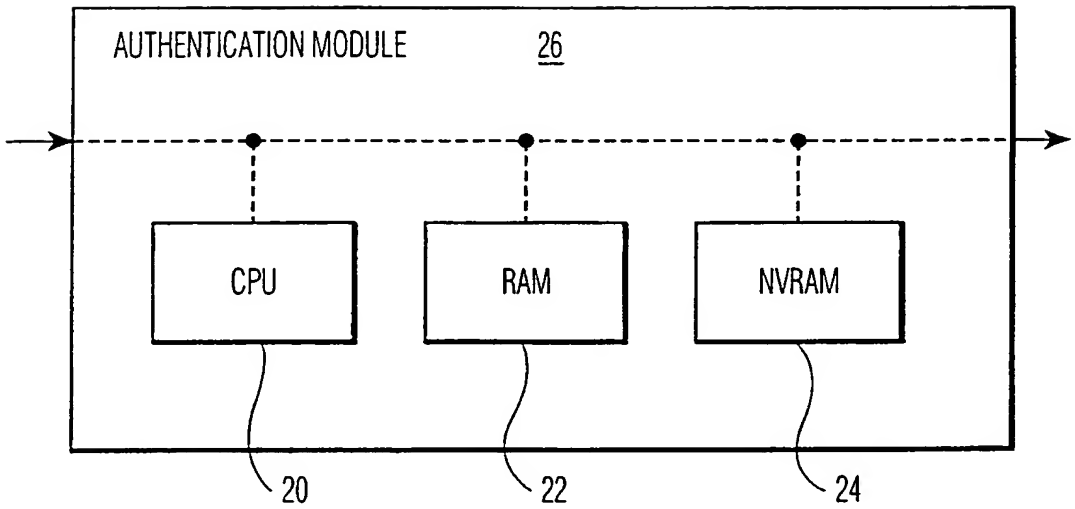


FIG. 2

INTERNATIONAL SEARCH REPORT

Intern· ·al Application No
PCT/EP 00/06371

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99 12088 A (WIEHLER GERHARD ;SIEMENS NIXDORF INF SYST (DE)) 11 March 1999 (1999-03-11) page 4, line 15 -page 14, line 2 figures 1-3	1-14
A	EP 0 714 204 A (LG ELECTRONICS INC) 29 May 1996 (1996-05-29) page 6, line 21 -page 11, column 2 figures 7-21	1-14

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 October 2000	31/10/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Van der Zaal, R

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

....ormation on patent family members

Intern· ıal Application No
PCT/EP 00/06371

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9912088 A	11-03-1999	AU 1020199 A	22-03-1999
		EP 1010052 A	21-06-2000
EP 0714204 A	29-05-1996	CN 1137723 A	11-12-1996
		JP 8242438 A	17-09-1996
		US 5757909 A	26-05-1998

Form PCT/ISA/210 (patent family annex) (July 1992)